CLAIMS

WHAT IS CLAIMED IS:

1. A device, comprising:

a port configured to receive at least one operating mode signal, wherein the at least one operating mode signal is indicative of a first operating mode;

one or more secured assets; and

security hardware coupled to receive the at least one operating mode signal, wherein the security hardware is further coupled to control access to the secured assets dependant upon the at least one operating mode signal.

2. The device of claim 1, further comprising:

at least one bus interface logic for coupling to a first external bus, wherein the one or more secured assets are coupled to the at least one bus interface logic.

3. The device of claim 2, wherein the at least one operating mode signal is received by the security hardware through the at least one bus interface logic.

4. The device of claim 1, wherein the one or more secured assets includes one or more of the group consisting of:

a random number generator,

a secure management register,

a monotonic counter, and

a secure memory.

5. The device of claim 1, wherein the first operating mode comprises system management mode.

6. The device of claim 1, wherein the security hardware includes:

an initiation register coupled to receive a request to change to the first operating mode; and

control logic coupled to the initiation register, wherein the control logic is configured to assert a control signal indicative of the request to change to the first operating mode, wherein the control signal initiates the change to the first operating mode.

7. The device of claim 6, wherein the control signal indicative of the request to change to the first operating mode comprises a system management interrupt.

8. The device of claim 1, wherein the security hardware includes:

a kick-out timer coupled to receive the at least one operating mode signal, wherein the kick-out timer is configured to output a signal indicating when the at least one operating mode signal is continuously active for at least a predetermined period of time.

9. The device of claim 8, wherein the kick-out timer is reset in response to a change in the at least one operating mode signal.

10. The device of claim 8, wherein the security hardware further includes:

a re-initiation timer coupled to receive the signal indicating when the at least one operating mode signal is active for the predetermined period of time, wherein the re-initiation timer is configured to output a signal indicating that another predetermined period of time has elapsed since the kick-out timer output the signal indicating when the at least one operating mode signal is continuously active for at least the predetermined period of time.

11. The device of claim 1, wherein the security hardware includes:

a duration timer coupled to receive the at least one operating mode signal, wherein the duration timer is configured to provide an indication of how long the at least one operating mode signal is active.

12. The device of claim 11, wherein the duration timer is reset in response to a change in the at least one operating mode signal.

13. The device of claim 11, wherein the security hardware further includes:

a kick-out timer coupled to the duration timer, wherein the kick-out timer is configured to output a signal indicating when at least one operating mode signal is continuously active for at least a predetermined period of time.

14. The device of claim 13, wherein the kick-out timer and the duration timer comprise a single timer.

15. The device of claim 13, wherein the security hardware further includes:

a re-initiation timer coupled to receive the signal indicating when the at least one operating mode signal is active for a predetermined period of time, wherein the re-initiation timer is configured to output a signal indicating that another predetermined period of time has elapsed since the kick-out timer output the indicating when the at least one operating mode signal is continuously active for at least the predetermined period of time.

16. The device of claim 1, wherein the security hardware includes:

access filters coupled to receive an indication when the at least one operating mode signal is active, wherein the access filters are configured to provide access requests to each of the one or more secured assets while the at least one operating mode signal is active, wherein the access filters are further configured to provide a predetermined response in lieu of data when the at least one operating mode signal is not active.

17. The device of claim 16, wherein the security hardware further includes:

access locks coupled to the access filters, wherein the access locks are further coupled to receive a mode signal, wherein the access locks are configured to disable the access filters in response to the mode signal indicating an unlocked mode.

18. The device of claim 1, wherein the security hardware includes:

mailbox RAM configured to store input and output data, wherein the mailbox RAM includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

19. The device of claim 18, wherein the input data for the one or more secured assets is addressed to the inbox of the mailbox RAM.

20. The device of claim 18, wherein the output data from the one or more secured assets is retrieved from an address at the outbox of the mailbox RAM.

21. The device of claim 18, wherein the security hardware further includes:

access filters configured to provide input data or access requests to the inbox of the mailbox RAM while the at least one operating mode signal is active, wherein the access filters are further configured not to provide input data to the inbox of the mailbox RAM when the at least one operating mode signal is not active, and wherein the access filters are further configured to provide a predetermined response in lieu of data upon receipt of said access requests when the at least one operating mode signal is not active.

22. The device of claim 21, wherein the security hardware further includes:

access locks coupled to the access filters, wherein the access locks are further coupled to receive a mode signal, wherein the access locks are configured to disable the access filters in response to the mode signal indicating an unlocked mode.

23. The device of claim 1, wherein the security hardware further includes:

scratchpad RAM, wherein each of the one or more secured assets is configured to access the scratchpad RAM for the storage of data.

24. The device of claim 1, further comprising:

a power port configured to receive at a reserve power signal, wherein the reserve power signal provides reserve power to the one or more secured assets.

25. The device of claim 1, further comprising:

a power port configured to receive a reserve power signal, wherein the reserve power signal provides reserve power to the security hardware.

26. The device of claim 1, wherein the device comprises a bridge, wherein the bridge further comprises:

first bus interface logic for coupling to a first external bus, wherein the one or more secured assets are coupled to the first bus interface logic; and

second bus logic for coupling to a second external bus, wherein the one or more secured assets are further coupled to the second bus interface logic.

27. The device of claim 26, wherein the bridge comprises a south bridge, wherein the first external bus is configurable as a first I/O bus, and wherein the second external bus is configurable as a second I/O bus.

28. The device of claim 26, wherein the first I/O bus is a PCI bus, and wherein the second I/O bus is an LPC bus.

29. The device of claim 1, wherein the device is comprised on a single integrated circuit.

30. A device, comprising:

first bus interface logic for coupling to a first external bus;

a port configured to receive at least one operating mode signal, wherein the at least one operating mode signal is indicative of a first operating mode;

one or more secured assets, wherein the one or more secured assets are coupled to the first bus interface logic; and

security hardware coupled to control the one or more secured assets, wherein the security hardware includes:

an initiation register coupled to receive a request to change to the first operating mode;

control logic coupled to the initiation register, wherein the control logic is configured to assert a control signal indicative of the request to change to the first operating mode, wherein the control signal initiates the change to the first operating mode;

a kick-out timer coupled to receive the at least one operating mode signal, wherein the kick-out timer is configured to output a signal indicating when the at least one operating mode signal is continuously active for at least a predetermined period of time;

a re-initiation timer coupled to receive the signal indicating when the at least one operating mode signal is active for a predetermined period of time, wherein the re-initiation timer is configured to output a signal indicating that another predetermined period of time has elapsed since the kick-out timer output the signal indicating when the at least one operating mode signal is continuously active for at least the predetermined period of time; and

access filters coupled to receive an indication when the at least one operating mode signal is active, wherein the access filters are configured to provide access requests to each of the one or more secured assets when the at least one operating mode signal is active, wherein the access filters are further configured to provide a predetermined response in lieu of data when the at least one operating mode signal is not active.

31 The device of claim 30, wherein the at least one operating mode signal is received by the security hardware through the at least one bus interface logic.

32. The device of claim 30, wherein the one or more secured assets include one or more of the group consisting of:

a random number generator,

a secure management register,

a monotonic counter, and

a secure memory.

33. The device of claim 30, wherein the first operating mode comprises system management mode.

34. The device of claim 30, wherein the control signal indicative of the request to change to the first operating mode comprises a system management interrupt.

35. The device of claim 30, wherein the security hardware includes:

a duration timer coupled to receive the at least one operating mode signal, wherein the duration timer is configured to provide an indication of how long the at least one operating mode signal is active.

36. The device of claim 35, wherein the kick-out timer and the duration timer comprise a single timer.

37. The device of claim 30, wherein the security hardware further includes:

access locks coupled to the access filters, wherein the access locks are further coupled to receive a mode signal, wherein the access locks are configured to disable the access filters in response to the mode signal indicating an unlocked mode.

38. The device of claim 30, wherein the security hardware further includes:

mailbox RAM configured to store input and output data, wherein the mailbox RAM includes an inbox for storing input data for the one or more secured assets and an outbox for storing output data from the one or more secured assets.

39. The device of claim 38, wherein the input data for the one or more secured assets is addressed to the inbox of the mailbox RAM.

40. The device of claim 38, wherein the output data from the one or more secured assets is retrieved from an address at the outbox of the mailbox RAM.

41. The device of claim 38, wherein the access filters are further configured to provide input data or access requests to the inbox of the mailbox RAM if the processor is operating in the secure operating mode, wherein the access filters are further configured not to provide input data to the inbox of the mailbox RAM if the processor is not operating in the secure operating mode, and wherein the access filters are further configured to provide a predetermined response in lieu of data upon receipt of said access requests if the processor is not operating in the secure operating mode.

42. The device of claim 30, wherein the security hardware further includes:

scratchpad RAM, wherein each of the one or more secured assets is configured to access the scratchpad RAM for the storage of data.

43. The device of claim 30, further comprising:

a power port configured to receive a reserve power signal, wherein the reserve power signal provides reserve power to the one or more secured assets and to one or more of the security hardware.

44. The device of claim 30, wherein the device comprises a bridge, wherein the bridge further comprises:

second bus logic for coupling to a second external bus, wherein the one or more secured assets are further coupled to the second bus interface logic.

45. The device of claim 44, wherein the bridge comprises a south bridge, wherein the first external bus is configurable as a first I/O bus, and wherein the second external bus is configurable as a second I/O bus.

46. The device of claim 45, wherein the first I/O bus is a PCI bus, and wherein the second I/O bus is an LPC bus.

47. A device, comprising:

means for interfacing with a first external bus;

means for receiving at least one operating mode signal, wherein the at least one operating mode signal is indicative of a first operating mode;

one or more secured means, wherein the one or more secured means are coupled to the means for interfacing with the first external bus; and

security means coupled to control the one or more secured means, wherein the security means include:

means for receiving a request to change to the first operating mode;

means for asserting a control signal indicative of the request to change to the first operating mode, wherein the means for asserting a control signal indicative of the request to change to the first operating mode initiates the change to the first operating mode;

means for receiving the at least one operating mode signal coupled to means for outputting a signal indicating when the at least one operating mode signal is continuously active for at least a predetermined period of time;

means for receive the signal indicating when the at least one operating mode signal is active for a predetermined period of time coupled to means for outputting a signal indicating that another predetermined period of time has elapsed since the means for outputting a signal indicating when the at least one operating mode signal is continuously active for at least a predetermined period of time

output the signal indicating when the at least one operating mode signal is continuously active for at least the predetermined period of time; and

means for filtering coupled to receive an indication when the at least one operating mode signal is active, wherein the means for filtering provide access requests to each of the one or more secured means when the at least one operating mode signal is active, wherein the means for filtering provide a predetermined response in lieu of data when the at least one operating mode signal is not active.

48 The device of claim 47, wherein the at least one operating mode signal is received by the security means through the means for interfacing with the first external bus.

49. The device of claim 47, wherein the one or more secured means include one or more of the group consisting of:

means for generating a random number generator,

means for providing a monotonic value, and

means for storing data.

50. The device of claim 47, wherein the security means further includes:

means for receiving the at least one operating mode signal coupled to means for providing an indication of how long the at least one operating mode signal is active.

51. The device of claim 47, wherein the security means further include:

means for locking the means for filtering, wherein the means for locking are coupled to receive a mode signal, wherein the means for locking disable the access filters in response to the mode signal indicating an unlocked mode.

52. The device of claim 47, wherein the security means further include:

means for storing input and output data, wherein the means for storing input and output data include a means for storing input data for the one or more secured means and a means for storing output data from the one or more secured means.

53. The device of claim 52, wherein the input data for the one or more secured means are addressed to the means for storing input data for the one or more secured means.

54. The device of claim 52, wherein the output data from the one or more secured means is retrieved from an address at the means for storing output data from the one or more secured means.

55. The device of claim 52, wherein the means for filtering comprise means for providing input data or access requests to the means for storing input data for the one or more secured means if the at least one operating mode signal is indicative of the first operating mode; means for blocking the input data from the means for storing input data for the one or more secured means if the at least one operating mode signal is not indicative of the first operating mode, and means for providing a predetermined response in lieu of data upon receipt of said

access requests if the at least one operating mode signal is not indicative of the first operating mode.

56. The device of claim 30, further comprising:

means for providing reserve power to the one or more secured means and to one or more of the security means.